

RAPPORT D'ACTIVITÉ 2012



41, avenue de la Gare · L-1611 Luxembourg

SMILE - home of:









RAPPORT D'ACTIVITÉ
2012

GROUPEMENT D'INTÉRÊT ÉCONOMIQUE "SECURITY MADE IN LËTZEBUERG" (SMILE)

SOMMAIRE

PRÉFACE



Etienne Schneider
Ministre de l'Économie et du Commerce extérieur

Assurer la sécurité des systèmes d'information et des données numériques est primordial afin d'évoluer en toute sérénité dans le monde de l'e-économie. Les grands groupes et entreprises du secteur des technologies de l'information et de la communication, tels que RTL Group, SES, mais aussi Amazon, iTunes, eBay, PayPal, Vodafone, Rakuten, Skype et bien d'autres, ont choisi le Luxembourg comme siège social pour leurs activités. Une des raisons pour ce choix est la qualité de nos infrastructures. Le Grand-Duché inspire confiance et fournit aux entreprises un environnement de sécurité fiable. Ces atouts doivent être développés en permanence si nous souhaitons rester dignes de notre bonne renommée gagnée au fil des années.

Préserver le niveau de confiance et de sécurité au sein de la société numérique représente un défi considérable. Les incidents qui se multiplient en fréquence, en envergure et en qualité ces derniers temps attirent l'attention du grand public ainsi que des entreprises actives dans ce domaine.

Contrairement aux idées reçues, la sécurité de l'information ne concerne pas seulement les grandes entreprises, mais également les PME. Un incident ou une panne technique, une fraude ou une attaque ciblée peuvent avoir des conséquences considérables sur le bon fonctionnement de l'entreprise, peu importe sa taille. La productivité et la confiance des clients, associés ou actionnaires peuvent être touchées et la survie de l'entreprise peut en dépendre.

Une société qui protège ses informations agit en bon père de famille à l'égard des ressources engagées et démontre au client qu'elle respecte les données qui lui sont communiquées. C'est un gage de confiance pour toutes les parties concernées.

C'est dans ce cadre que je salue le rôle croissant, depuis sa création en 2010, du groupement d'intérêt économique (G.I.E.) Security made in Lëtzebuerg - SMILE, qui par le biais de ses trois piliers BEE SECURE, CASES et CIRCL, œuvre efficacement pour la sensibilisation du grand public aux bons réflexes en matière d'utilisation d'Internet, pour la formation des employés d'entreprises et d'administrations aux risques et solutions inhérents aux systèmes d'information, ainsi que pour la prévention et la gestion d'incidents au niveau national.

2012 aura été une année importante pour SMILE : l'initiative BEE SECURE a lancé avec succès sa campagne de sensibilisation au cyber-harcèlement intitulée « NOT FUNNY BEE FAIR - Stop cybermobbing ». Ce thème est également abordé sur l'année 2012-2013 dans les établissements scolaires grâce aux enseignements dispensés par des formateurs labellisés.

CIRCL pour sa part a géré dans l'année 2012 environ 7000 investigations techniques et incidents relatifs à la sécurité de l'information, ce qui représente une augmentation considérable par rapport à l'année précédente. CASES s'est consacré prioritairement à l'évolution de sa mission auprès des PME/TPE en développant la plateforme myCASES. Cette dernière est un espace « B2B » complémentaire au nouveau site Internet www.cases.lu permettant aux entreprises d'accéder aux différents niveaux d'outils et de services d'analyse de risques et de recevoir les conseils de spécialistes en sécurité de l'information, afin de mieux protéger leurs activités.

Je suis persuadé que les initiatives entreprises par les structures telles que SMILE contribueront à accroître nos compétences en matière de sécurité des systèmes de l'information, tout comme la prise de conscience de nos responsabilités - et par là à renforcer l'engagement du Luxembourg dans l'économie numérique.

Etienne Schneider
Ministre de l'Économie et du Commerce extérieur

SMILE



INTRODUCTION



« SMILE » a pour ambition de s’établir comme intervenant-clé dans l’amélioration de la sécurité de l’information au Luxembourg et de constituer un lien fort entre le secteur privé et les organismes publics. Des partenariats sont développés continuellement pour renforcer le soutien accordé à la sécurité de l’information appliquée à l’économie. L’union avec les communes, par l’intermédiaire du SIGI et du SYVICOL d’un côté, et les contacts avec des prestataires de services de sécurité de l’autre, permettent à SMILE de représenter un centre d’excellence répondant à une demande croissante, en créant de nouveaux marchés et en poursuivant la promotion des coopérations internationales.

Pascal Steichen

Directeur général du groupement d’intérêt économique
« Security made in Lëtzebuerg » (SMILE)



MEMBRES



L'Etat du Grand-Duché de Luxembourg, représenté par les ministères de la Famille et de l'Intégration, de l'Éducation nationale et de la Formation professionnelle et de l'Économie et du Commerce extérieur, ainsi que les syndicats SIGI (Syndicat Intercommunal de Gestion Informatique) et SYVICOL (Syndicat des Villes et Communes du Luxembourg) ont fondé et gèrent en partenariat SMILE g.i.e. Ce groupement d'intérêt économique est issu de la nécessité de préserver au sein d'une structure permanente, les résultats et activités développés dans le cadre des initiatives BEE SECURE, CASES et CIRCL. Son fonctionnement et ses objectifs reposent sur le « plan directeur de la sécurité des systèmes d'information et de la communication » [1] défini par le Ministère de l'Économie et du Commerce extérieur et s'inscrivent depuis 2012 dans la nouvelle démarche du « Cyber Security Board » au Ministère d'Etat : la « Stratégie nationale en matière de cyber sécurité »[2].







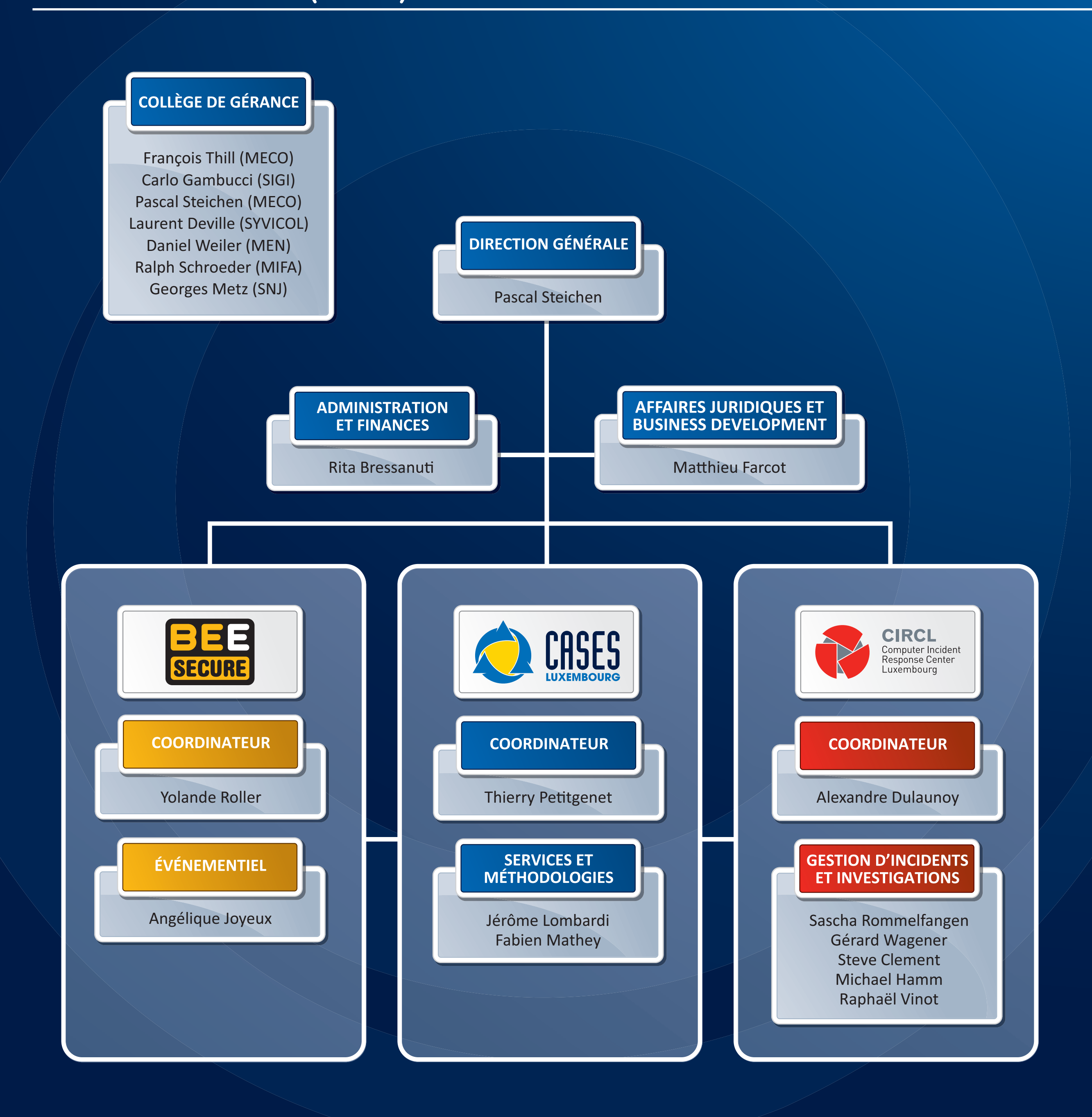




[1] http://www.eco.public.lu/attributions/dg2/d_communications/commerce_electronique/plan_directeur/index.html

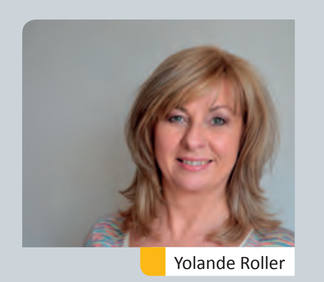
[2] http://www.mediacom.public.lu/cybersecurity/Strat__gieCybersecurity_122011.pdf

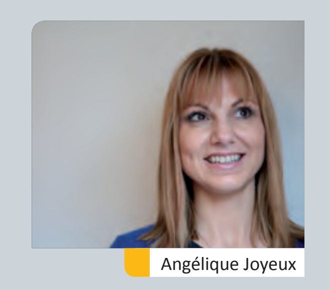
ORGANISATION (2013)




Pascal Steichen


Rita Bressanutti


Yolande Roller

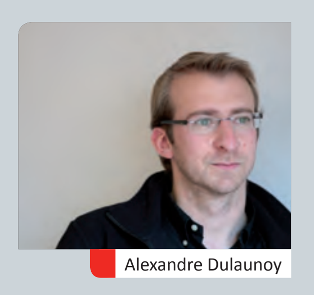

Angélique Joyeux

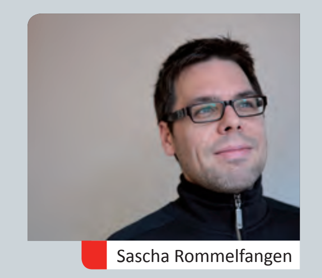

Matthieu Farcot

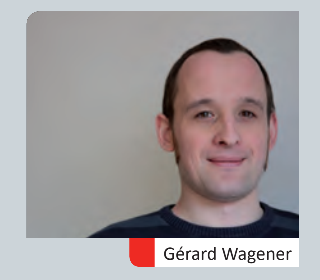

Thierry Petitgenet


Jérôme Lombardi

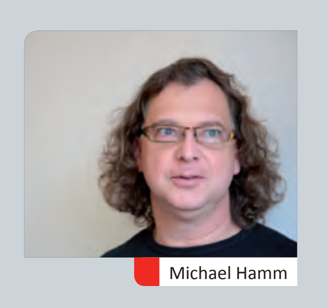

Fabien Mathey


Alexandre Dulaunoy


Sascha Rommelfangen


Gérard Wagener


Steve Clement


Michael Hamm


Raphaël Vinot

PÔLES D'ACTIVITÉS

BEE SECURE - « la sensibilisation et l'éducation du grand-public » :

encourager les citoyens et plus particulièrement les enfants, les jeunes et les seniors à profiter des nouvelles technologies de l'information et de la communication en toute confiance et de façon sécurisée.

CASES (Cyberworld Awareness Security Enhancement Services) - « la démocratisation des méthodologies et des bonnes pratiques » :

analyser les risques et innover dans les méthodologies mises en place dans les politiques de sécurité, favoriser les collaborations sur le marché en proposant un rôle de facilitateur et de coordinateur pour les projets rattachés à la sécurité, contribuer à l'élaboration de standards et d'un cadre législatif adapté aux besoins, aussi bien sur le plan national qu'international, représenter une expertise de référence sur le marché de la sécurité de l'information (technique et juridique).

CIRCL (Computer Incident and Response Center Luxembourg) - « la réaction rapide et l'analyse après incident informatique » :

développer et renforcer les compétences d'intervention face aux incidents de sécurité touchant aux réseaux et systèmes d'information des membres, de leurs partenaires et du secteur privé en général, promouvoir et participer à des programmes de recherche en matière de sécurité de l'information en partenariat avec des acteurs internationaux ou nationaux, dont l'université du Luxembourg et les centres de recherche publics.

PRÉSENCE MÉDIAS

Une dizaine de communiqués de presse et une trentaine d'articles et dossiers sont parus dans la presse écrite. Quelques quinze interviews radio sur RTL Radio Lëtzebuerg, Eldoradio, Radio Latina, 100,7 et DNR, ainsi que deux reportages télé sur RTL Télé Lëtzebuerg ont assuré la présence de BEE SECURE, CASES respectivement CIRCL dans les médias en 2012.

PRÉSENCE SUR LES RÉSEAUX SOCIAUX

	SITE INTERNET	TWITTER	FACEBOOK	YOUTUBE
BEE SECURE	90 visites/jour	260 followers	1 170 fans	6 300 visualisations
CASES	180 visites/jour	900 followers	260 fans	1.600 visualisations[1]
CIRCL	642 visites/jour[2]	424 followers	n/a	n/a

[1] Depuis janvier 2013 [2] Ceux-ci incluent les rapports d'incidents faits via le formulaire en ligne

PROJECTS

FESTIVAL ON STÉITSCH

„BEE AWARE – Think before you share"

Überlege Dir genau, welche Fotos Du im Internet veröffentlichst. Warum? Das wirst Du bei dieser Aktion zum Thema Bildrechte erfahren... Doch Vorsicht: Schock-Gefahr! :) Übrigens, auch die ZAP-Fotolounge ist wieder am Start!

Kampagne "NOT FUNNY – BEE FAIR"

Bei On Stéitsch startet die neue BEE SECURE Kampagne zum Thema Cybermobbing. „NOT FUNNY", denn bei Cybermobbing hört der Spaß im Netz nämlich auf! Es ist unfair, illegal und auch nicht so anonym, wie die meisten denken... deshalb der Aufruf „BEE FAIR".

Wer davon betroffen ist, sollte unbedingt mit einer Vertrauensperson sprechen oder die BEE SECURE Helpline zu Rate ziehen unter der Telefonnummer: 26 64 05 44

Du bass den Expert. Schwätz mat !

Dein Handy ist dein wichtigster Begleiter? Du interessierst Dich für das Thema Sicherheit im Netz? Dann mach mit beim „BEE SECURE Youth Panel"! Wir treffen uns einmal im Monat, z.B. beim Pizzaessen, Musikmachen oder im Hochseilgarten. Wer Lust hat, meldet sich ganz einfach über das Kontaktformular auf www.bee-secure.lu. Wir freuen uns auf Dich!

Facebook Lounge

Wie auch im letzten Jahr, lädt die BEE SECURE Facebook-Lounge zum Chillen und Surfen ein. Wer will, kann auf einer übergroßen Facebook-Wall mitposten! Es gibt auch eine analoge Wall zum Anfassen ... lass dich überraschen.

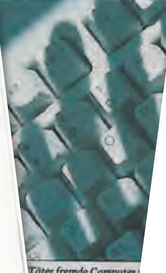




„Bee Secure" warnen vor Be...

Phishing

...et oder persönlich um Hera...



Täter fremde Computer...

Sortir couvert

ICT

Les entreprises doivent analyser leur exposition aux dangers pour réu... de prévention des risques informatiques pertinente et performante. Re...

Vincent Ruck (texte), Olivier Minaire (photo)



François Thill (Cases) : « *La mise en pratique des standards est laborieuse et discriminatoire du point de vue de la complexité.* »

La connexion généralisée a rendu les entreprises beaucoup plus exposées aux risques de piratage informatique. C'est un jeu permanent entre les responsables informatiques, qui cherchent à améliorer leur protection, et les hackers, qui cherchent à passer outre tous les murs. La question, pour de nombreuses structures, reste en fait de bien comprendre les risques auxquels elles sont exposées.

Pour soutenir cet effort, la communauté internationale a répondu à de nombreuses questions en matière de méthodologies sécuritaires, via la famille des normes ISO 2700x, qui les guide dans la gouvernance de sécurité. Le standard ISO/IEC 27001 définit, par exemple, un modèle servant à la mise en place d'un système de management de la sécurité de l'information. ISO/IEC 27002 définit, lui, un code de bonnes pratiques pour la gestion de la sécurité de l'information. Enfin, ISO/IEC 27005 propose un modèle d'analyse de ri...

Pour François ... et du Comme... recourir à ces... laborieuse et ...

complexité. Ainsi, chaque approche spécifique, analy... effectuer une veille des... même émergentes. » D'o... méthodologiques de Cases... responsable : « *Sans les e... serait impossible pour une... en la matière de suivre l'é... des menaces et vulnérabili...*

Quoi qu'il en soit, il e... continuellement son niv... *de la mise en place de m... et techniques, il ne faut... compte le facteur huma... dispenser une formation... portement adéquat.* »

Approches ... pou...

ICT

« DU PRAGMATISME »

La sécurité informatique n'est pas qu'une question de technologie. Elle est aussi – surtout ? – une question de prudence et de bonnes pratiques individuelles.

ICT & Innovation

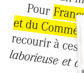
« ACQUÉRIR UNE VISION G...

La sécurité des systèmes d'information peut être plus efficace si elle est réalisée en collaboration avec d'autres structures, par des échanges d'informations et de bonnes pratiques.

Interview Vincent Ruck Photo Olivier Minaire

Neuer Name, gleiches Konzept

Lisa Stopline heißt jetzt Bee Secure Stopline



LES PIÈGES DU WEB DOSSIER 3

«Impossible de tout contrôler»

Vol de données, prolifération de virus et espionnage : en dix ans, les cybercriminels ont sensiblement renforcé leur stratégie. Et ils deviennent de plus en plus difficiles à repérer. Manuel Silvoso, expert en informatique et collaborateur de l'initiative Bee Secure du ministère de l'Économie, explique pourquoi.

Entretien avec notre journaliste Christiane Kleer



Manuel Silvoso de Bee Secure, appelle à la méfiance sur la Toile.

Photo : archives lq/Isabella Finzi

L'utilisateur lambda peut-il se sentir en sécurité quand il surfe sur le net?

Manuel Silvoso : On n'est jamais sûr sur le web. Or, ce qui est sûr, c'est que de nombreux services proposés sur le web sont gratuits. On peut donc dire que les avantages d'internet contrebalancent ses désavantages. En effet, les personnes derrière ces sites doivent être payées, notamment grâce à la pub. Et pour ce faire, toutes nos données sont enregistrées, qu'il s'agisse de nos mails, de nos commentaires sur les réseaux sociaux ou des sites que nous visitons. Ces données permettent d'établir des profils de consommateur et sont donc exploités par les publicitaires. On peut évidemment dire que c'est affreux, mais c'est plus ou moins légitime.

Peut-on contourner cette stratégie des publicitaires?

Non, mais pour moi, la devise est : respecte les règles où ne joue pas. Ceux qui se plaignent du manque de protection chez Facebook n'ont qu'à fermer leur ...

pédopornographiques ou racistes peut avertir la Lisa Stopline. Les sites proposant des programmes illicites peuvent être signalés au Circl (Computer Incident Response Center Luxembourg). Ces démarches partent en gros de l'initiative de l'utilisateur.

Ne peut-on pas envisager une police du web?

Les collaborateurs du Circl essaient déjà de jouer un rôle proactif dans ce domaine. À l'aide de certains indicateurs, ils essaient de dépister les sites frauduleux. Or, le problème, c'est le nombre de sites, c'est de la prolifération sauvage, impossible de tout contrôler! Et surtout : grâce à des moyens techniques, l'anonymat complet est tout à fait possible sur le web, ce qui fait qu'il devient très difficile de retrouver les cybercriminels. Certaines études montrent d'ailleurs...

Les serveurs du FBI, qui permettaient l'accès à Internet des adresses IP touchées, ser...

De 250 à 300 ordinateurs du Luxembourg peu... black-out complet dans les semaines à venir. E... conséquences du virus DNSChanger vont se fai... À cette date, les adresses IP infectées par le pro... été redirigées par le FBI, seront coupées, suite à...

VIRUS «DNSCHANGER»

02 juillet 2012 16:24; Act:

Vous risquez de perd... Internet le 9 juillet

Dernier délai pour vérifier que son ordinateur n'est pas i... le virus «DNSChanger». Sinon, le 9 juillet, près de 300 p... luxembourgeois risquent de ne plus avoir accès à Interne...

LOGICIEL AU LUXEMBOURG

07 novembre 2012 16:20; Act: 07.11.2012 17:22

Attention aux faux mails de la police

LUXEMBOURG - Un nouveau logiciel malveillant s'attaque aux ordinateurs en se faisant passer pour une action anti-piratage menée par la police du Grand-Duché.



...warnt PC-Nutzer

...melden sich über Telefon

...einem schlimmen Virus infiziert, denn in der Tat spielen sich dank der Fremdmanipulation aus der Ferne unheimliche Dinge am heimischen Bildschirm ab. Die Betrüger ziehen dann ihr Ass aus dem Ärmel: Wenn eine gewisse Geldsumme bezahlt wird, kann der vermeintlich infizierte Computer via Windesleife repariert werden. Im schlimmsten Fall wird das Opfer dabei allerdings nicht nur seines Geldes und seiner Daten beraubt, sondern es entstehen auch noch hohe Reparaturkosten, um den Computer von den Schadprogrammen, beziehungsweise Trojaner zu befreien.

Die Betrüger selbst agieren in der Regel aus dem ferneren Ausland. Wurden die Opfer anfangs fast ausschließlich auf Englisch kontaktiert, haben sich die Anrufe längst weitere Sprachkenntnisse angeeignet. So liegen Fälle, in denen Holländisch und Deutsch gesprochen wurde, vor. Eine Kontaktaufnahme auf Deutsch ist ebenfalls wahrscheinlich.

Wer einen Anruf von angeblichen Computerexperten erhält, der ihn auf Probleme mit seinem PC hinweist, sollte den Aufforderungen auf keinen Fall nachkommen und das Gespräch sofort beenden. Bei Fragen ... CASES mit einem Kontaktformular auf www.cases.lu ... Wer an technischen Fragen interessiert ist, kann sich auch an CIRCL, das nationale (Computer Emergency ...)

...Betrugsmasche wurden. Die Angreifer kontaktieren ihre Opfer per Telefon und geben sich als Experten großer internationaler Firmen, wie etwa Microsoft, aus. In oft langen Gesprächen wird das Opfer dann vorgegaukelt, sein PC von Schadprogrammen infiziert ist. Die Angreifer nutzen die Angst des Opfers aus, um es auf eine Fernwartungswebsite (zum Beispiel www.logmein.com) oder www.... zu locken, unter dem Vorwand, hier aus werde man sich um die Beseitigung des Virus kümmern.

In Wahrheit handelt es sich dabei allerdings um eine üble Betrugsmethode. Mit ihrem Einloggen auf diesen Fernwartungsseiten überlassen die Opfer den Angreifern nämlich den uneingeschränkten Zugriff auf den heimischen Computer und damit auf die Einsicht in persönliche und Bankkonten. In der Regel installieren die Angreifer Trojaner auf dem Computer und erlangen so die komplette Kontrolle ...

BEE SECURE



INTRODUCTION



Le succès de l'initiative BEE SECURE repose aussi sur l'équipe compétente et dévouée de SMILE. Avec SMILE nous pouvons compter sur un partenaire fort.

Eric Krier

*Service National de la Jeunesse, **Responsable BEE SECURE***

SMILE g.i.e. collabore avec le SNJ (Service National de la Jeunesse) au sein de l'initiative BEE SECURE. Celle-ci englobe les actions communes du Ministère de l'Economie et du Commerce extérieur, du Ministère de la Famille et de l'Intégration et du Ministère de l'Education nationale et de la Formation professionnelle en matière de sensibilisation à une utilisation plus sécurisée des technologies de l'information et de la communication du grand public (enfants, jeunes, parents, professeurs, éducateurs, seniors, etc.). Les actions envers les enfants, les jeunes ainsi qu'envers leur entourage sont cofinancées par la Commission Européenne dans le cadre du programme « Safer Internet Plus ».

En 2012, BEE SECURE a largement développé son engagement en augmentant sensiblement ses actions d'information en direction du grand public et de formation des différents intervenants. L'initiative est à l'origine de nombreuses activités et projets coordonnés, avec toujours le souci de formuler son message en fonction du contexte et du public visé. Cette faculté d'adaptation permet à un large public de profiter des savoirs et savoir-faire en matière de sécurité de l'information et contribue à faire naître et à étendre une « culture de la sécurité » dans l'utilisation des nouveaux médias.

KANNERJUGENDTELEFON



SMILE travaille en étroite collaboration avec les psychologues et pédagogues du KannerJugendTelefon (KJT) qui proposent une écoute et une aide aux enfants et jeunes, facilement accessible via le **116 111**, ainsi qu'aux parents via le « Elterentelefon ».

La structure s'occupe également de la **BEE SECURE Helpline** destinée au grand public et aux éducateurs et qui informe et conseille en matière d'usages des technologies de communication.

Enfin, le KJT s'engage avec la **BEE SECURE Stopline** (anciennement LISA Stopline) qui lutte contre les contenus Internet à caractère illégal en signalant de façon anonyme les incidents suspects aux forces de l'ordre, que ce soit au Luxembourg ou à l'étranger. Les domaines de compétences couverts sont les abus sexuels sur mineurs, le racisme, la discrimination, le révisionnisme et le terrorisme.

CAMPAGNES ET ÉVÉNEMENTS D'ENVERGURE

BEE SECURE a participé à de nombreux événements tout au long de l'année. Près de 18 concerts et festivals pour jeunes ainsi que 15 foires et manifestations destinées au grand public ont été couverts. Un bref aperçu :

- Elaboration de la **campagne nationale de sensibilisation : « NOT FUNNY BEE FAIR – Stop cybermobbing »,** officiellement lancée lors de la manifestation « On Stéitsch » en septembre 2012 où plus de 1 400 visiteurs étaient présents.

Le but est de promouvoir un comportement fair-play et responsable dans l'utilisation des TIC, mais aussi d'informer sur les diverses aides disponibles pour lutter contre le cyber-harcèlement.

La campagne annuelle remplit 3 objectifs : éduquer de manière positive, créer une culture de la sécurité et instaurer une vue élargie des problématiques inhérentes au thème de la sécurité de l'information.

Grâce au soutien de plus de 25 partenaires, l'affichage de 3 200 posters, la distribution de plus de 20 000 flyers d'information et la distribution de 15 000 balles anti-stress et 20 000 bracelets de l'amitié, la campagne de sensibilisation 2012-2013 remplit la mission d'utilité publique qui lui a été confiée.

- Coordination de la campagne **« Eastereggs and Toothbrushes »**, un projet transnational avec la Commission européenne en partenariat avec l'Irlande et la Roumanie destiné à analyser, entre autres, la tendance des luxembourgeois à divulguer leur mot de passe ou autres informations personnelles à une personne inconnue.

L'étude menée avec le support de l'Université de Luxembourg a révélé que sur les 1 200 personnes interrogées dans 3 villes du Grand-Duché, 2/3 d'entre elles dévoilent des données sensibles en échange de quelques chocolats.



■ **Safer Internet Day** luxembourgeois sur le thème « Connecting generations » lors duquel ont été organisées 3 conférences à la Maison de l'Europe et au Cercle Cité.

■ Présence au **Postlaf** organisé par les P&T Luxembourg où 250 personnes sont passées sur le photo lounge BEE SECURE pour être sensibilisés au droit à l'image, ceci grâce à la prise de photos-portraits manipulées pour les besoins de la campagne.

■ Participation à la **foire d'automne** à Luxexpo, au cours de laquelle le stand BEE SECURE a attiré 5 000 visiteurs. Le stand illustrait la thématique de la campagne de sensibilisation grand public 2012-2013 : « NOT FUNNY BEE FAIR - Stop cybermobbing ». Cet événement était également un important soutien au **Cyber Security Month**, événement créé au niveau européen par l'**ENISA**.

■ Participation à la **foire de l'étudiant** où a été réalisée la sensibilisation de 2 500 jeunes sur le thème du cybermobbing.

■ Soutien de la Fondation Cancer avec une équipe de sportifs lors de la manifestation **« Relais pour la vie »** où près de 9 000 personnes sont passées sur le stand d'approvisionnement sponsorisé par BEE SECURE.

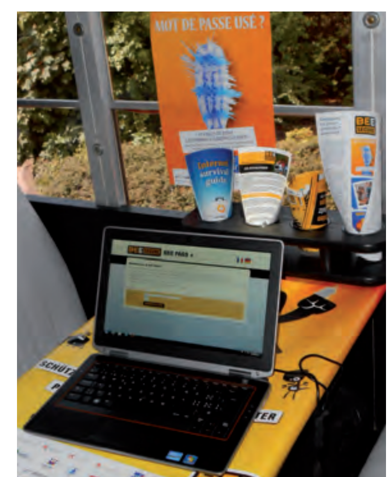
■ Animation d'un stand étape lors de la manifestation **« Rallye Nichtrauchen »** réunissant plus de 1 000 jeunes lycéens et fournissant des conseils sur les bons réflexes à adopter sur Internet.

■ Organisation et animation de *« l'Université BEE SECURE »* dans les villages d'enfants **« Mini-Hesper »** à Hesperange et **« Mini Lenster »** à Junglinster.

NB : La liste intégrale des événements est disponible sur le site BEE SECURE.









SERVICES D'INFORMATION ET DE SUPPORT GRAND-PUBLIC

Le portail BEE SECURE www.bee-secure.lu, dédié au grand-public, a été entièrement repensé pour améliorer son ergonomie et simplifier son accès. En 2012, le portail a été largement enrichi et propose de nombreux contenus et actualités thématiques expliquant les concepts et approches servant à sécuriser son ordinateur et ses données.



■ On y trouve également de nombreuses ressources pédagogiques pour parents et enseignants : https://www.bee-secure.lu/fr/ressources/publications

■ À côté des événements et de la présence Internet, BEE SECURE propose des services publics dédiés, tels :







Quelques supports de sensibilisation :

■ Brochure « Pièges à éviter » en version FR, DE, EN, PT
En collaboration avec l'ULC (Union luxembourgeoise des consommateurs).

■ Facebook - Leitfaden für Eltern en version DE

■ **Quizz en ligne spécial « BEE PASS » consacré au cyber-bullying** et destiné aux jeunes, permettant ainsi de vérifier leurs connaissances en la matière, version DE et FR.
https://beepassspecial.bee-secure.lu/



FORMATIONS EN MATIÈRE D'USAGE DES MÉDIAS ÉLECTRONIQUES

Les **BEE SECURE Trainings**, obligatoires pour l'enseignement secondaire, sont proposées aux écoles fondamentales aussi bien qu'à un public de parents d'élèves, d'enseignants ou tout autre groupe sur demande. En fonction du public cible et de ses desideratas, les formateurs BEE SECURE disposent de nombreuses sessions de sensibilisation en 5 versions linguistiques : FR, LB, EN, DE, ES. Leur évaluation est réalisée par l'Université de Luxembourg.

Le Luxembourg est le seul pays d'Europe à avoir mis en place une formation obligatoire au sein de l'enseignement. Le financement des formations est majoritairement réalisé par le Ministère de l'Education nationale et de la Formation professionnelle. La coordination des formateurs et des rendez-vous est assurée par le Service National de la Jeunesse.
Fin 2012, SMILE a mis en place un label pour s'assurer en continue de la qualité des formateurs BEE SECURE.

QUELQUES CHIFFRES

380 classes de 7e des lycées classiques et techniques formées, soit l'entièreté de cette population.

180 classes de l'enseignement fondamental des cycles 3 et 4, représentant plus de 10 000 jeunes formés.

40 soirées d'information pour parents.

12 formations pour multiplicateurs, représentant plus de 200 instituteurs et éducateurs impliqués.

30 séances dans le cadre du secteur jeunesse (maisons relais et maisons de jeunes), représentant 250 jeunes sensibilisés.




NOT FUNNY
BEE FAIR
Tipps
Internet sicherer
CASES

CASES



INTRODUCTION



L'année 2012 aura représenté une étape décisive dans la conceptualisation des nouveaux objectifs de CASES. À l'aube de notre 10ème anniversaire en 2013, l'année écoulée a permis de préparer l'avènement du nouveau CASES : « Cyberworld Awareness and Security Enhancement **SERVICES** »

François Thill

Ministère de l'Économie et du Commerce extérieur, ***Responsable CASES***

Créé en 2003 par la volonté du ministère de l'Économie et du Commerce extérieur de sécuriser les systèmes d'information au Luxembourg, la « Cyberworld Awareness and Security Enhancement Structure » s'adressait dès ses débuts à un large public, composé de professionnels et de personnes privées, d'employés d'administrations luxembourgeoises, de personnel éducatif, de parents et de jeunes. En 2008, elle fut épaulée dans sa mission par la création de CIRCL, le « Computer Incident Response Center Luxembourg », responsable de la veille technologique et de la gestion d'incidents. À côté de CASES et CIRCL, diverses autres initiatives[3] émanant notamment des Ministères de la Famille et de l'Intégration, de l'Éducation nationale et de la Formation professionnelle œuvraient dans le domaine de l'éducation au bon usage des nouveaux médias.

La consolidation en 2010 de l'ensemble des efforts de sensibilisation du grand public sous l'initiative BEE SECURE coordonnée par le Service National de la Jeunesse, ainsi que la création du groupement d'intérêt économique SMILE regroupant les projets CASES, CIRCL et BEE SECURE ont été des étapes importantes en vue d'une structuration des tâches, respectivement de la réorientation des objectifs et du public cible de CASES.

Ainsi, la formation aux médias électroniques du personnel scolaire, tout comme la sensibilisation des parents et des jeunes sont dorénavant orchestrées principalement par l'initiative BEE SECURE. CIRCL quant à lui a été reconnu au niveau international en tant que CERT national (« Computer Emergency Response Team ») responsable de la veille technologique et de la gestion d'incidents, en étroite coopération avec les deux autres CERT luxembourgeois[4].

[3] My SecureIT, LuSI, Lisa-Stopline, et toutes autres activités luxembourgeoises supportées par le programme européen « Safer Internet »

[4] GOVCERT.LU (www.govcert.lu) et RESTENA-CSIRT (www.restena.lu/csirt)

L'équipe CASES se consacre dorénavant prioritairement à sa mission d'accompagnement à la sécurité de l'information des entreprises (PME/TPE), des administrations et des ministères luxembourgeois. Mandaté par ailleurs depuis 2012 par le « Cyber Security Board », CASES sensibilise les agents de l'État luxembourgeois aux risques liés à l'utilisation des technologies d'information et de communication en coopération avec l'Institut national d'administration publique (INAP).

La simplification des méthodologies de sécurité de l'information, ainsi que l'expérience inédite dans l'application d'outils de gestion des risques et de la mise en place de politiques de sécurité, font partie du savoir-faire qui est mis au service des organismes professionnels. 2012 a permis de développer un ensemble d'outils adapté aux nouveaux besoins et de tester la plateforme technique y associée, notamment auprès de certaines communes luxembourgeoises.

DEUX NOUVELLES PLATEFORMES EN LIGNE : WWW.CASES.LU ET MY.CASES.LU

Le site CASES, considéré depuis sa création comme ressource essentielle en matière de sécurité de l'information au Luxembourg, risquait de devenir au fil du temps et de la thématique grandissante une source de « surinformation ». L'année 2012 a donc vu une réorganisation des sujets traités, une mise à jour des textes et documents, ainsi qu'une restructuration de l'arborescence et du « look » du site.

L'utilisateur peut dorénavant s'initier de manière simple et exhaustive aux bons réflexes pour une utilisation responsable des médias électroniques. Le site présente plus d'une centaine d'articles comprenant à la fois des explications techniques, comportementales et organisationnelles, auxquels s'ajoutent de nombreux guides de bonnes pratiques et des documents illustrant une approche méthodologique de la sécurité de l'information.



Le nouveau site présente 3 niveaux de navigation :

- Vous avez une question relative à l'utilisation d'Internet ou de l'e-mail ? La section « SOS - Besoin d'aide ? » vous guidera vers l'explication adéquate.
- Vous souhaitez prévenir ou traiter un risque ? La section « RISQUES » décrit de manière exhaustive les mesures à prendre.
- Vous souhaitez maîtriser la sécurité ? Consultez la section « MAITRISE ».

Par ailleurs les rubriques « News » et « Alertes » tiennent l'utilisateur au courant des événements notables en matière de sécurité de l'information et informent sur les grands risques informatiques touchant le Grand-Duché.

L'année 2012 a en particulier servi à la création d'un espace B2B sécurisé **« myCASES »**, fondamentalement novateur dans son concept et parfaitement intégré à la philosophie CASES et donc au site www.cases.lu.

Les services « myCASES » permettent une maturation pragmatique et progressive de la sécurité de l'information au sein d'un organisme (la démarche myCASES prévoit 3 niveaux consécutifs). Cette plateforme « web » propose des outils sectoriels et sert comme point d'échange dans le cadre de missions d'accompagnement aux organismes désireux de procéder à une évaluation des risques sur leurs systèmes d'information, de recevoir du matériel de sensibilisation adapté à leurs besoins ou de procéder au développement d'une politique de sécurité personnalisée.





my.cases.lu

En 2012 CASES a réalisé une quinzaine d'évaluations dans le secteur public (communal) et privé. Ces analyses ont contribué à la finalisation de l'outil intégré d'analyse sectorielle des risques au sein de la plateforme **« myCASES »**.

Le lancement officiel de « myCASES » qui sera accessible via https://my.cases.lu/ est prévu pour l'été 2013.

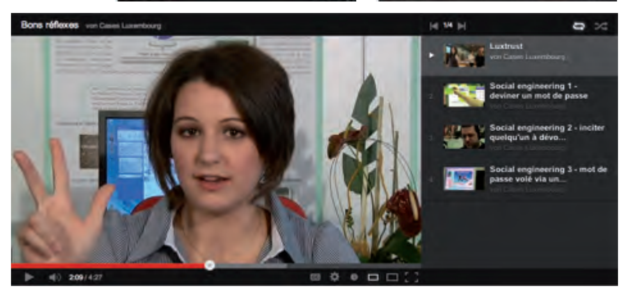
FORMATIONS ET SENSIBILISATIONS

CASES sensibilise également son public par le biais de formations ou de films thématiques, tels que diffusés par exemple sur http://youtube.cases.lu/

Des formations s'adressant spécifiquement aux agents de la fonction publique ont été organisées pour *le service des Médias et des Communications, pour les porte-parole du gouvernement luxembourgeois à l'étranger, pour l'institut national d'administration publique (INAP)*, pour *le Conseil d'État, pour l'institut luxembourgeois de régulation (ILR)* ainsi que pour la *commune d'Ettelbrück*, première commune au Luxembourg à sensibiliser la totalité de son personnel administratif.







PRÉSENTATIONS ET PARTICIPATION AUX CONFÉRENCES

Au niveau événementiel, quatre workshops relatifs à la sécurité de l'information et à l'analyse de risques ont eu lieu au Grand-Duché, en particulier pour le **« Paperjam business club »** ainsi que pour les communes luxembourgeoises dans le cadre du **« SIGI DAY »**.

En septembre 2012, CASES a invité les spécialistes du marché à faire un état des lieux inédit en matière de sécurité de l'information. La journée **« La sécurité au cœur de l'information »**, était l'occasion pour une vingtaine de sociétés spécialisées et plus de 150 participants d'échanger leurs expériences et connaissances dans le domaine de la sécurité de l'information.

A cela s'ajoute une **trentaine de présentations** effectuées dans le cadre de diverses demandes professionnelles.
Sur le plan international, CASES a été l'hôte de la conférence gouvernementale **« Vis!t 2012 »**. Une soixantaine d'experts en sécurité de l'information venus d'Autriche, de Suisse, d'Allemagne et du Luxembourg se sont réunis au Grand-Duché pour partager leurs expériences et discuter des nouvelles tendances en la matière.



Les dix dernières années CASES a su s'affirmer en tant que partenaire de confiance pour les professionnels, aidé en cela par sa plateforme d'information : www.cases.lu.
Plus d'informations seront disponibles dans une brochure dédiée aux 10 ans CASES à paraître en 2013.

CIRCL



INTRODUCTION



De nos jours l'omniprésence de l'IT est telle qu'il n'est plus suffisant de se protéger au mieux, il faut se préparer à réagir aux attaques auxquelles nous sommes tous régulièrement exposés. CIRCL, les « pompiers d'Internet » remédie aux attaques et traite le cas échéant les incidents informatiques.

Pascal Steichen

Ministère de l'Économie et du Commerce extérieur, ***Responsable CIRCL***



CIRCL[7] (CERT national) est l'équipe d'intervention nationale qui répond aux incidents de sécurité informatique du secteur privé et des administrations communales luxembourgeoises, ainsi que le point de contact international pour toutes les questions qui y sont relatives. L'équipe opérationnelle de CIRCL (6 personnes) est hébergée par le g.i.e. SMILE. Le cas échéant, deux ressources supplémentaires sont à disposition au Ministère de l'Economie et du Commerce extérieur.

En 2011, CIRCL avait traité 4 453 événements[8]. En 2012, CIRCL en a traité 10 852, dont plus de 1 000 investigations techniques[9] réparties sur les secteurs d'activités majeurs du Grand-Duché.

[7] Computer Incident Response Center Luxembourg

[8] Un événement est assimilé à une entrée dans la base de données CIRCL. Ceci peut être généré par des outils de sécurité automatisés (p. ex. des « honeypots »), rapporté par un partenaire national ou international ou bien directement par une entité du Grand-Duché.

[9] Une grande partie des événements est traitée de manière automatisée. Parmi ceux qui sont à traiter manuellement, CIRCL définit comme « investigation technique » les cas qui nécessitent au moins un jour-homme de travail d'analyse.

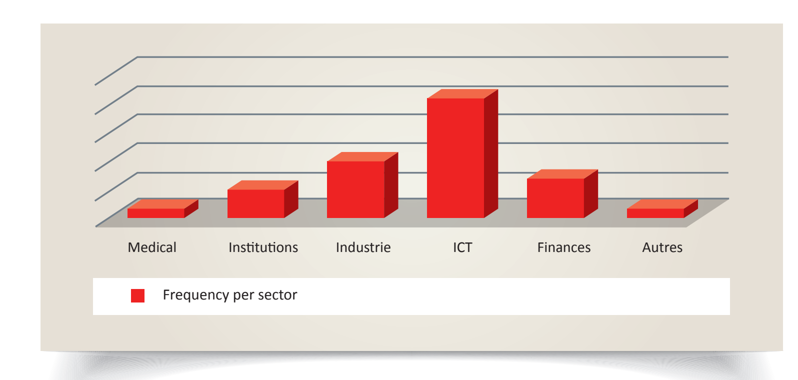


Figure 2: Fréquence des événements traités par CIRCL, par secteur (source: CIRCL 2011)

La progression continue du nombre d'attaques enregistrée par CIRCL (phénomène similaire dans la plupart des pays du monde[10]) est principalement liée au fait que les outils de détection, les échanges entre entités de type CERT[11] ainsi que la volonté de rapporter des incidents deviennent de plus en plus fréquents et performants. Elle ne s'explique donc pas uniquement par une recrudescence du nombre d'incidents.
De nouvelles catégories de menaces sont apparues en 2012, montrant une évolution des attaques ciblant plus spécifiquement les personnes privées.

Au travers des analyses d'incidents, CIRCL a pu identifier les tendances suivantes au niveau des menaces :

- l'abus d'infrastructures « web » non ou mal sécurisées, en particulier :
  - des CMS (p.ex. Joomla, Wordpress, Drupal...) mal configurés
  - des « plugins navigateurs »[12] vulnérables
- l'ingénierie sociale[13], via :
  - des techniques d'abus de confiance[14] et d'arnaques (p.ex le cas des « scammeurs Microsoft »[15])
  - des « chevaux de Troie », comme le « ransomware policier »[16]
- la mauvaise gestion des multiples vulnérabilités dans « Java »[17]
- les systèmes ICS/SCADA[18] mal configurés et utilisés comme rebonds d'attaques

[10] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
[11] Computer Emergency Response Team, terme générique pour une entité comme CIRCL
[12] http://fr.wikipedia.org/wiki/Plugin
[13] http://fr.wikipedia.org/wiki/Ing%C3%A9nierie_sociale_%28s%C3%A9curit%C3%A9_de_l%27information%29
[14] http://fr.wikipedia.org/wiki/Abus_de_confiance
[15] https://www.cases.lu/des-scammeurs-contaminent-les-ordinateurs-prives.html
[16] https://www.cases.lu/information_police_themed_ransomware.html
[17] http://fr.wikipedia.org/wiki/Java_(technique)
[18] http://fr.wikipedia.org/wiki/Supervisory_Control_and_Data_Acquisition

Les motivations des attaques sont catégorisées par CIRCL de la manière suivante :

- à but financier (communément appelées « cyber-criminalité ») - **(50%)**[19]
- à but géopolitique ou avec du soutien gouvernemental - **(30%)**
- à but ludico-politique (ou « cyber-activisme ») - **(20%)**

Au-delà des activités de support aux victimes d'attaques informatiques, CIRCL participe activement à la communauté « sécurité » nationale et internationale.

CONFÉRENCES ET PARTENARIATS

En octobre 2012, CIRCL, en collaboration avec le CSRRT-LU, a organisé la 8ème édition de la conférence internationale hack.lu. Cette conférence s'est établie comme rencontre incontournable pour tout professionnel du domaine de la sécurité informatique du Luxembourg et de la Grande-Région, mais a également gagné en visibilité par-delà cette zone.

CIRCL a été impliqué, tant par des présentations sur des thèmes d'actualités que par sa participation active, dans de multiples rencontres internationales dont : TF-CSIRT, FIRST, CERT-Verbund, ainsi que dans plusieurs conférences de sécurité internationales de haut niveau (p. ex. DEFCON, Blackhat, CCC, Hackito-Ergo-Sum…).

CIRCL a su renforcer son positionnement en tant que partenaire et point de contact privilégié pour le Luxembourg dans la communauté « sécurité » et « CERT » internationale, tout en initiant et gardant des liens établis et des collaborations bilatérales fortes avec l'Autriche, la Belgique, les Etats-Unis, les Pays-Bas, la France, l'Inde et la Russie.

CIRCL contribue activement, en étroite collaboration avec le CERT-EU, à la sécurisation des institutions européennes présentes sur le territoire luxembourgeois. Plus spécifiquement, CIRCL est un des fondateurs du groupe de travail européen sur la recherche et l'analyse de « malware »[20].

[19] Le pourcentage est assimilé à la charge de travail d'analyse de l'équipe CIRCL en jour-homme
[20] Terme regroupant les virus, vers, chevaux de Troie et autres codes malicieux
[21] https://www.circl.lu/pub/tr-07/
[22] https://www.circl.lu/pub/tr-09/
[23] https://www.circl.lu/report/
[24] https://www.circl.lu/files/CIRCL-trendreport-2011.pdf

PUBLICATIONS, OUTILS ET R&D

Suivant l'actualité et des besoins spécifiques, CIRCL publie des dossiers ou rapports de fond sur des thématiques de pointe sur son site Internet - www.circl.lu.
Les publications les plus intéressantes en 2012 :

- HOWTO pour identifier les en-têtes (« headers »), indispensables à l'analyse et au retraçage d'e-mails[21]
- Tutoriel sur la détection et le nettoyage potentiel de « malware »[22]
- Guide pratique sur la manière de rapporter un incident de manière efficiente[23]
- Rapport 2010-2011 sur les menaces et tendances en sécurité informatique du Luxembourg[24]
- Site dédié à la détection du malware « DNS Changer » - **www.dns-ok.lu**

En collaboration avec quelques universités nationales et internationales, CIRCL a participé activement à diverses publications scientifiques et contribue à une dizaine de projets de recherche.

Pour faire face au nombre d'incidents croissant, CIRCL développe des outils automatisant les tâches journalières de gestion d'incidents pouvant aussi servir à d'autres professionnels :

- **nfdump-tools** - un outil d'analyse de grandes quantités de données de type « network flows »
- **pe32-cert-dump** - un outil pour extraire des certificats de fichiers binaires de type « PE »
- **vt-tools** - pour l'automatisation de requêtes sur « VirusTotal »
- **bgp-ranking** - pour établir le niveau de confiance d'un FAI et analyser son évolution
- **traceroute-circl** - un outil améliorant les fonctionnalités de base de « traceroute » pour la recherche d'information technique sur Internet
- **cve-search** - outil de recherche dans la base des vulnérabilités mondiales CVE
- **IP-ASN-history** - outil d'historisation des appartenances IP/ASN
- **lnf-tools** - outil « big data » netflow
- **alod** - outil de détection d'indices de compromission pour Mac OS X

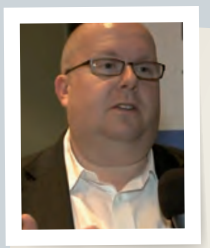
Ces outils sont publiquement accessibles et distribués sous licence libre.

SMILE VU PAR D'AUTRES



"Le Luxembourg a manifesté une volonté très claire d'agir sur le plan de la sécurité lié aux technologies de l'information. (...) C'est cette dynamique qui fait la différence entre le Luxembourg et d'autres pays".

Bertrand Lathoud, Paypal



"Créer la confiance en Internet et les NTIC en général est notre devoir".

Marco Houwen, dclux



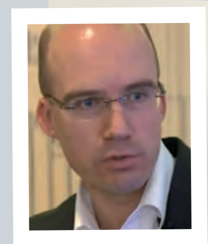
"Aujourd'hui, les vulnérabilités sont de moins en moins du côté du de la technique et de plus en plus du côté humain. L'humain est le point faible !".

Eric Chassard, PWC



"Ce que nous devrions définitivement être prêts à faire c'est défendre nos infrastructures, nos institutions et nos applications, afin que nous puissions continuer à vivre de manière normale. C'est extrêmement important"

Steve Purser, ENISA



"La sécurité internet est comme jouer au chat et à la souris. Il y aura toujours une nouvelle menace à laquelle faire face et nous devrons être capables de réagir le plus rapidement possible".

Xavier Buck, eurodns



"Nous devons anticiper, nous devons éviter, nous devons intervenir et nous devons réagir pour faire face aux dangers liés à l'utilisation des nouveaux medias ".

François Biltgen,
Ministre des Communications et des Médias

HISTORIQUE DE SMILE

SENSIBILISATION ET ACCOMPAGNEMENT POUR ORGANISMES

CASES LUXEMBOURG

2003
Création de **CASES** (Cyberworld Awareness and Security Enhancement Structure)

2004
Mise en ligne de **www.cases.public.lu**

2005
CASES reconnu **"bonne pratique"** par l'ENISA

2006
Premier mode d'emploi pour PME/PMA sur la **politique de sécurité**

2007
Campagne **"e-commerce en toute sécurité"** en partenariat avec l'ABBL

2008
"Secure MJ" politiques de sécurité et formations pour maisons de jeunes

2009
Première campagne nationale sur la protection des données : **"À poil sur la toile"**

2010
"Meet the hackers" première conférence "info sec" pour décideurs

SENSIBILISATION DE LA POPULATION LUXEMBOURGEOISE

2003
Début de **"My SecureIT"** (sensibilisation dans les écoles)

2006
Création de **LUSI** (Luxembourg Safer Internet)

LUSI Luxembourg Safer Internet

2008
Création de **LISA-StopLine**

LISA Stop Line Luxembourg Internet Safety Alert

2009
Memorandum of Understanding entre 3 ministères en vue de renforcer et de coordonner les initiatives "Safer Internet" (LUSI & LISA) par le SNJ (Service National de la Jeunesse)

2010
Consolidation des activités et services sous un même sigle : **BEE SECURE**

BEE SECURE

GESTION D'INCIDENTS ET RECHERCHE

CIRCL Computer Incident Response Center Luxembourg

2008
Création de **CIRCL** (Computer Incident Response Center Luxembourg)

2010
5 ETP de **SMILE g.i.e.** dédiés pour CIRCL

2011
Mandat officiel de **CERT national** et **accréditation TI**

2010/11



- une joint-venture entre plusieurs entités du Grand-Duché de Luxembourg
- une seule plateforme pour promouvoir une culture de la sécurité de l'information
- des services adaptés à 4 domaines de la sécurité de l'information :
  - la prise de conscience ;
  - la prévention des risques ;
  - la réaction aux incidents ;
  - la recherche et le développement.



www.bee-secure.lu · info@bee-secure.lu

BEE SECURE Helpline : (+352) 26 64 05 44
BEE SECURE Stopline : stopline.bee-secure.lu
BEE SECURE Trainings : www.bee-secure.lu/formulaire
facebook.com/beesecure
twitter.com/beesecure
youtube.com/beesecureTV
podcast.bee-secure.lu



www.cases.lu · help@cases.lu

my.cases.lu
twitter.cases.lu
youtube.cases.lu
facebook.cases.lu
gplus.cases.lu
linkedin.cases.lu



www.circl.lu · info@circl.lu

Tél : (+352) 24 78 84 44
Anonymous reporting: www.circl.lu/contactform/
twitter.com/circl_lu



www.smile.public.lu · info@smile.public.lu

41, avenue de la Gare · L-1611 Luxembourg
Tél.: (+352) 27 40 09 86 01